We already have several decode events and rules but there are still some missing. For example we have the `stream.reassembly_overlap_different_data` stream event and rule for that but we're missing the one for `stream.reassembly_overlap` where we have just the `tcp.overlap` counter.

At least those are missing:
- `tcp.reassembly_gap`
- `tcp.overlap`
- `tcp.insert_data_normal_fail`
- `tcp.insert_data_overlap_fail`
- `tcp.insert_list_fail`

I guess this might be a bigger task to collect all possible events.

For every event there should be a rule in the rules/*-events.rules files.

But `tcp.reassembly_gap` is covered by `tcp.reassembly_gap` so that's not missing.

If I look into `StreamTcpThreadInit` where we register the counter I see also some where it's quite obvious that we don't want to trigger an event for every `StatsIncr` of those.

I guess there is no easy way to determine which ones are missing beside the overlap and insert fails. It might be enough to cover those which we found and add even more if someone spots a missing one that might be handy for debugging.

That's why I stumbled upon that, while I wanted to dig into why there are sometimes high `tcp.overlap` values and with a rule it would help to narrow it
Thoughts?

#7 - 09/24/2019 08:40 PM - Andreas Herz
- Assignee changed from Community Ticket to Andreas Herz

#8 - 09/26/2019 08:31 AM - Victor Julien
Lets just add the missing ones, but commented out by default.

#9 - 10/21/2019 08:35 PM - Andreas Herz
- Status changed from New to Assigned